UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/785,849	02/16/2001	Hans Christopher Sowa	CM04816H	2108

22917 7590 12/07/2005

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER	
BLUDAU, BRANDON S	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/785,849	SOWA ET AL.	
	Examiner	Art Unit	
	Brandon S. Bludau	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application filed 2/16/2001; amendment filed 5/09/2005.

2. Claims 1-22 are pending. Claims 23 – 164 are withdrawn from consideration. Claim 1 is an independent claim.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 20 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 20 discloses a method of decrypting the encryption key of claim 1. However, it is noted that neither in claim 1 or claim 19 is the first encryption key said to have been encrypted which would require the subsequent decryption disclosed in claim 20.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claims 1,10,15,18 are rejected under 35 U.S.C. 102(a) as being anticipated by Roelofsen ("TETRA Security").

6. As per claim 1, Roelofsen discloses a method comprising the steps of:

Generating, by a first system device, a first encryption key;

Forwarding the first encryption key from the first system device to a second system device;

Storing the first encryption key at the second system device (page 50 paragraph 8 wherein the first encryption key is the Group Cipher Key (GCK) and the second system device is the MS.)

7. As per claim 10, Roelofsen discloses the method of claim 1, further comprising the step of encrypting the first encryption key with an interkey (page 51 paragraph 1), yielding a first encrypted encryption key;

Forwarding the first encrypted encryption key to a fourth system device (Page 51 paragraph 1 wherein the fifth device is an MS unit);

Decrypting, by the fourth system device, the first encryption key into the first encryption key (page 51 paragraph 1 wherein each MS can decrypt the key using the authentication key for the MS page 50 paragraph 2).

8. As per claim 15, Roelofsen discloses the method of claim1, further comprising the steps of:

Encrypting the first encryption key with a key associated with a mobile station, yielding an encrypted mobile encryption key;

Forwarding the mobile encryption key to the mobile station (page 51 paragraph 1 and page 50 paragraph 2 wherein the key identifies the handset and thus is associated with a mobile station).

9. As per claim 18, Roelofsen discloses the method of claim 1, further comprising the step of encrypting the first encryption key with an interkey prior to the forwarding step (page 50 paragraph 4 and page 51 paragraph 5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 2-4,6-8, 11-14,16,17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roelofsen, and further in view of Hakim (US Patent 4841433).

11. As per claim 2, Roelofsen discloses the method of claim 1, further comprising the steps of:

Forwarding the second encryption key to a third system device (page 50 paragraph 5 wherein the second key is the Derived Cipher Key).

Roelofsen does not disclose generating a second encryption key by combining the first encryption key with a third encryption key

Hakim does disclose generating a derived cipher key by combining a first key with a third key (column 4 lines 1-15).

Hakim is analogous art because it discloses a method for using keys to authenticate a user for access to some entity.

It would have been obvious to one of ordinary skill in the art to modify Roelofsen to include generating the second key by combining a first key and a third key.

Motivation to modify Roelofsen as discussed above would have been to provide an authentication system wherein the key contains the original information of the subkeys to permit access to groups of different entities as implied in Hakim column 4 and 5 and in the abstract.

12. As per claim 3, Roelofsen discloses the method of claim 2, wherein the third system device is any of a base station, a base site, and TETRA site controller (page 50 paragraph 5 wherein the Derived Cipher Key is used for uplink communications, thus implying the DCK is at the network, i.e. base station), wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station residing at any of the base station, the base site, and the TETRA site controller when the first encryption key is generated (page 50 paragraph 5 wherein it is well known in the art of mobile communication networks that authentication between the network and the mobile station requires the mobile station to access the DCK as noted in the paragraph and thus the network station wherein the mobile station resides would receive the authentication key), and wherein the mobile station is affiliated with a talkgroup associated with the first encryption key (page 50 paragraph 8 1st sentence wherein the first encryption key is the GCK).

13. As per claim 4, Roelofsen discloses the method of claim 2, wherein the third system device is any of a base station, a base site, and a TETRA site controller, wherein the step of forwarding the second encryption key to a third system device is

triggered by a mobile station arriving at any of the base station, the base site, and the TETRA site controller, and wherein the mobile station is affiliated with a talkgroup associated with the first encryption key (the same rejection for claim 3 follows here, it is well known in the art of mobile communication systems that a key needed to authenticate a mobile station would be sent to the base station as a particular mobile station arrives at a base station).

14. As per claim 6, Roelofsen discloses the method of claim2, wherein the third encryption key is associated with the third system device (page 50 paragraph 6 wherein the third encryption key is the Common Cipher Key (CCK) and the third system device is the network station connected to the geographical area as understood in the art).

15. As per claim 7, Roelofsen discloses the method of claim 2, wherein the third encryption key is a common cipher key (page 50 paragraph 6).

16. As per claim 8, Roelofsen discloses the method of claim 2, further comprising the step of communicating over an air interface by encrypting messages with the second encryption key (page 50 paragraph 5 wherein the second encryption key is the DCK and is used to encrypt the link between the network and the MS).

17. Claim 11 is rejected because it discloses the same subject matter as claim 2.

18. As per claim 12, Roelofsen discloses the method of claim 11, wherein the second encryption key is encrypted with an intrakey prior to being forwarded to the fifth system device (page 50 paragraph 4 lines 1-5 and page 51 paragraph 5).

19. Claim 13 is rejected because it discloses the same subject matter as claim 6.

20. Claim 14 is rejected because it discloses the same subject matter as claim 7.

21. As per claim 16, Roelofsen discloses the method of claim 15, further comprising the steps of:

Decrypting, by the mobile station, the encrypted mobile encryption key with the key associated with the mobile station, yielding the first encrypted key (page 50 paragraph 4 and wherein the user can generate the key for decryption page 50 paragraph 2);

Combining the first encryption key with a predetermined encryption key, yielding an air interface key (rejected in claim 3 wherein the predetermined key is the Common Cipher Key of Roelofsen page 50 paragraph 6);

Communicating over an air interface by encrypting messages with the air interface key (page 51 paragraph 2).

22. As per claim 17, Roelofsen discloses wherein the predetermined encryption key is a common cipher key (page 50 paragraph 6 and page 51 paragraph 2).

23. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roelofsen in view of Hakim (US Patent 4841433) and further in view of Jackson (US Patent 6477387).

Roelofsen discloses the method of claim 2, wherein the third system device is any of a base station, a base site, and a TETRA site controller, but does not disclose wherein the step of forwarding the second encryption key to a third system device is triggered by a mobile station changing talkgroup affiliation while residing at any of the base station, the base site, and the TETRA site controller, and wherein the mobile

station changes talkgroup affiliation to a talkgroup associated with the first encryption key.

Jackson discloses wherein an encryption key associated with a talkgroup is sent to a device when triggered by a change in talkgroup wherein the key is for the new talkgroup (column 14 lines 16-28).

Jackson is analogous art because it discloses a method for grouping communication units in a communication system.

It would have been obvious for one of ordinary skill in the art to modify Roelofsen to include a step of sending an encryption key for a new talkgroup when a mobile unit changes to the new talkgroup.

Motivation for one to modify Roelofsen as discussed above would have been for enabling secure communication for the user changing talkgroups, as discussed by Jackson in column 14 lines 22-26.

24. Claims 9,22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roelofsen in view of Hakim (US Patent 4841433) and further in view of Roelofsen ("Security Issues for TETRA Networks").

25. As per claim 9, Roelofsen ("TETRA Security") discloses the method of claim 2, but does not disclose wherein it is further comprising the step of updating the first encryption key when an encryption period associated with the third encryption key expires.

Roelofsen ("Security Issues for TETRA Networks") does disclose the step of updating the first encryption key when an encryption period associated with the third encryption key expires (section 3.2).

Roelofsen is analogous art because it discloses methods of securing a TETRA network.

The author is the same for both articles and both specifically discuss security implementation in TETRA networks, so obviousness for one of ordinary skill in the art to combine and motivation to combine are inherent.

26. As per claim 22, Roelofsen ("Security Issues for TETRA Networks") discloses the method of claim 1, further comprising the step of updating the first encryption key when an encryption period associated with the first encryption key expires (section 3.2).

Obviousness and motivation to combine are applied as in claim 9.

27. Claims 19,20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roelofsen in view of Marshall (US Patent 4888800).

28. As per claim 19, Roelofsen discloses the method of claim 1, but does not disclose it further comprising the step of acknowledging receipt of the first encryption key.

Marshall does disclose a method of acknowledging receipt of an encryption key (column 11 lines 19-40).

Marshall is analogous art because it is directed towards a method of distributing encryption keys.

It would have been obvious for one of ordinary skill in the art to modify Roelofsen to include the step of acknowledging the receipt of the encryption key.

Motivation for one to modify Roelofsen as discussed above would have been to ensure that the encryption key is received by the agent thus enabling secure communication in the future as is well known by one of ordinary skill in the art.

29. As per claim 20, Marshall discloses the step of claim 19, wherein the step of acknowledging comprises decrypting the first encryption key, and when the first encryption key is decrypted properly, generating an acknowledgment to be forwarded via an air traffic router to the first system device (column 11 lines 19-40).

Marshall is analogous art because it is directed towards a method of distributing encryption keys.

It would have been obvious for one of ordinary skill in the art to modify Roelofsen to include the step of acknowledging the receipt of the encryption key when the encryption key is decrypted properly.

Motivation for one to modify Roelofsen as discussed above would have been to ensure that the encryption key is properly received by the agent thus enabling secure communication in the future as is well known by one of ordinary skill in the art.

30. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roelofsen in view of Chang (US Patent 5329573).

Roelofsen discloses the method of claim1, but does not disclose wherein the second system device contains a home location register associated with the first encryption key.

Chang does disclose wherein the second system device contains a home location register associated with the first encryption key (column 2 lines 3-32).

Chang is analogous art because it is directed to managing authentication data in a telecommunications network.

It would have been obvious by one of ordinary skill in the art to modify Roelofsen to include a home location register at the second system device.

Motivation for one to modify Roelofsen as discussed above would have been to include a common device in telecommunication networks that is responsible for verifying and enabling legitimate routing of calls and ensuring security as would have been well known at the time to one of ordinary skill in the art.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon S Bludau
Examiner
Art Unit 2132

BB

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100